Montgomery County Council
Montgomery County, Maryland

Amendment #2 to
Request for Proposals #425820958

RFP Issue Date – August 20, 2015

Amendment #1 Issue Date – September 18, 2015

Amendment #2 Issue Date – October 8, 2015

Closing Date – October 16, 2015

This is an amendment to the Montgomery County Council's RFP #425820958. Section J – Computer Resources Security, on page 39 of the RFP refers to Attachment H to the RFP, which includes:

- Administrative Procedure 6-1 – Use of County-Provided Internet, Intranet, and E-mail Services
- Administrative Procedure 6-7 – Information Resources Security
- Computer Security Guideline (September 2004 version)

Attachment H was inadvertently excluded from the RFP document that has been available online on the Office of Legislative Oversight's website. An updated version of the RFP that includes Attachment H is now posted online. In addition, the RFP refers to the County's Computer Security Guideline (September 2004 version). The current version of the Computer Security Guideline is dated 2009 and is included in the updated RFP document.

Please call or email Leslie Rubin in the County Council's Office of Legislative Oversight at (240) 777-7998 or leslie.rubin@montgomerycountymd.gov with questions.

Copies of the RFP and of this Supplement can be found at www.montgomerycountymd.gov/olo.

Proposals must be received by <u>3:00 p.m.</u> on <u>October 16, 2015</u>.

Attachment H

MONTGOMERY COUNTY ADMINISTRATIVE PROCEDURE

Offices of the County Executive • 101 Monroe Street • Rockville, Maryland 20850

NO. 6-1

PAGE 1 OF 8

DATE 9/2/10

TITLE

Use of County-Provided Internet, Intranet, and E-mail Services

CAO APPROVAL

PURPOSE

1.0 To establish an administrative procedure governing the use of County-provided Internet, intranet, and electronic mail services by County employees. The County maintains intranet and Internet access for its employees for the purpose of improving productivity, professional development, and the level of service to the people of our community.

DEFINITIONS

2.0 Department of Technology Services (DTS) - A department in the executive branch that is responsible for automated information systems and telecommunications technology.

2.1 CIO - Chief Information Officer and DTS Department Head

2.2 Personal Use – Activity that is conducted for purposes other than accomplishing official or otherwise authorized activity.

POLICY

3.0 Internet, intranet, and electronic mail (email) services are provided to County employees and persons legitimately affiliated with the business of the County government for the efficient exchange of information and the completion of assigned responsibilities that are consistent with the County's purposes.

3.1 Employees must use County-provided Internet, intranet, and email services responsibly and professionally, and must not use Internet, intranet, or email services in a manner that violates any applicable federal, State, or Montgomery County law, regulation, or policy, including those contained in the County's Administrative Procedures.

3.2 A County employee may use County-provided Internet, intranet, or email services for personal purposes on only a limited, reasonable basis, and in accordance with this administrative procedure. However, employees must act reasonably to minimize personal use of County-provided Internet, intranet, and email services. Personal use of County Internet, intranet or email services by employees should mainly be during personal time (before and after work or during lunch time). Such use must be kept to a minimum, must not increase or create additional expense to the County and must not disrupt the conduct of service or performance of official duties.

3.3 An employee's use of County-provided Internet, intranet, or email services indicates consent to this administrative procedure, and to the County's access and monitoring, for legitimate business purposes (including a non-investigatory work-related search or investigatory search of suspected work-related misfeasance), of his/her electronically stored email messages and computer files, and any other data related to the employee's use of the County's Internet, intranet, and email services.

3.4 Any employee who is in violation of this administrative procedure may be subject to disciplinary action, including dismissal, and other legal remedies available to the County, in accordance with applicable federal, State, or Montgomery County laws and regulations, including Personnel laws and Regulations, and Ethics Laws, currently codified at Chapter 33, Appendix F, and Chapter 19A of the County Code, respectively, and applicable collective bargaining agreements, as amended.

GENERAL

CONNECTING TO INTERNET, INTRANET, AND EMAIL SERVICES

4.0 County employees may connect to County-provided Internet, intranet, or email services only through:

A. Personal Computers (PCs) such as desktops and laptops connected to the County's computer network via the County's secure enterprise Internet service connection; or

B. Stand-alone (non network-connected or temporarily disconnected) PCs via a private Internet Service Provider (ISP), such as America On-Line (AOL), or via a DTS-sanctioned remote access method.

4.1 Any PC that connects to County-provided Internet, intranet, or email services must have up-to-date antivirus software and current updates for Windows operating system software installed on it and must be configured to actively protect against virus infections and periodically scan the PC to check for viruses.

4.2 Costs incurred by the County for ISP connections to stand-alone PCs are the responsibility of the using department. Employees must obtain department approval prior to obtaining a County-provided ISP connection.

PROHIBITED USER CONDUCT

4.3 Employees must use County-provided Internet, intranet, and email services in accordance with this administrative procedure and all applicable laws, regulations, and policies. Prohibited conduct, including personal use, includes:

A. Accessing, sending, forwarding, storing, or saving on County PCs or servers any material that is offensive, demeaning or disruptive, including messages that are inconsistent with the County's policies concerning "Equal Employment Opportunity" and "Sexual Harassment and Other Unlawful Harassment," for any reason other than for purposes of eliminating this type of material from County systems. The act of inadvertently opening an email that contains this type of material does not, itself, constitute a violation of this policy.

B. Personal use beyond that permitted by this policy.

C. Any use prohibited by federal, State, or County law.

D. Employees may not modify computer equipment for personal purposes. This would include loading of personal software, non-County supplied software; "shareware" and/or "freeware"; animated (executable) screen savers or peer-to-peer software packages. Examples of inappropriate personal configuration include adding unauthorized wireless network cards, use of external storage devices that contain applications, and communications or video components not supplied or tested by the County.

E. Using the County's Internet, intranet, or email services to gain unauthorized access to County or other system resources.

F. Using the County's Internet, intranet, or email services for gambling or other illegal or County-prohibited activities.

G. Using the County's Internet, intranet, or email services for private gain or profit.

H. Infringing upon computer software and data protected by copyright intellectual property rights and/or license laws.

I. Using the County Internet, intranet, or email services or applications to publish and/or represent (expressly or implicitly) personal or unofficial opinions as those of the County.

J. Any personal use that could cause congestion, delay or disruption of service to any County system or equipment. This may include, but not limited to:

1. "Chain" or unnecessary "Reply All" emails; and
2. Downloads of video, sound or other large, non-work related files.

K. Sending broadcast messages to all, or the majority of, County e-mail users without obtaining prior approval from the Chief Administrative Officer (CAO), in accordance with County information technology policies and procedures.

COUNTY OWNERSHIP, MONITORING, CONTROL, AND DISCLOSURE

4.4 All County-provided electronic systems, hardware, software, temporary or permanent files and any related systems or devices used in the transmission, receipt or storage of Internet, intranet, or email communications are the property of, or licensed to, the County.

4.5 Any information transmitted or received by employees using the County's Internet, intranet, and email services, or stored on the County's computer resources, is the property of the County and, therefore, is not considered private. This includes email from an employee's personal account, such as Hotmail or AOL, if that email is stored on the County's computer resources.

4.6 Internet, intranet, and email electronic files and messages may be retrieved from storage by the County and its agents without prior notice to an employee, even if the electronic files and messages have been deleted by the sender or receiver. These messages and files may also be used by the County in disciplinary or other proceedings.

4.7 Employees must take appropriate measures to prevent unauthorized access to confidential information when using the County's Internet, intranet, and email services, in accordance with applicable federal, State, or Montgomery County laws, regulations, or policies regarding confidential information.

4.8 The County may monitor an employee's use of County-provided Internet, intranet, and email services, and may access an employee's email messages and computer files in its sole discretion, when there is a legitimate business purpose (including a non-investigatory work-related search or investigatory search of suspected work-related misfeasance). This includes access to email messages from an employee's personal email account, such as Hotmail or AOL, if the personal email is stored on the County's computer resources.

4.9 Upon the approval of the email user's department head and the CIO, system administrators in DTS or the email user's department may access an employee's email messages and computer files related to the employee's use of the County's Internet, intranet, and email services. The existence of privately held passwords and "message delete" functions do not restrict or eliminate the County's ability or right to access this information.

4.10 The County may monitor or control the flow of Internet/intranet and email traffic over the County's network for security or network management reasons, or for other legitimate business purposes.

4.11 The County may be compelled to access and disclose to third parties messages sent over its Internet, intranet, or email systems, in accordance with the Maryland Public Information Act (MPIA), Maryland Code Ann., State Gov't §§ 10-611 to 10-628 (1998 Repl. Vol.). The MPIA applies to an electronically stored email message or a hard copy of the message in the custody and control of a public officer or employee, if the message is related to the conduct of public business. 81 Op. Att'y Gen, Op No. 96-016, 1996 WL 305985 (1996).

RESPONSIBILITIES

5.0 Department of Technology Services

A. Provide a 24-hour, 7 day-a-week secure, high-speed enterprise connection to Internet, intranet, and email services.

B. Notify users of County-provided Internet, intranet, and email services when those services will be unavailable for system or network maintenance.

C. Provide operating system and anti-virus software for all County-owned PCs, and manage software configurations, including operating system and anti-virus, for all County-owned PCs connected to the County's network.

D. Accept help desk calls when a County employee or department notes a problem with County-provided Internet, intranet, or email services, and distribute information, updates, and/or resolutions, as appropriate.

E. Maintain the current version of this administrative procedure, in accordance with Administrative Procedure 6-6, Information Technology Policies and Procedures Manual.

F. Provide CIO approval or denial of a department head's request to monitor an employee's use of County-provided Internet, intranet, and email services, or to access an employee's email messages and computer files.

G. Provide information to a department head regarding an employee's use of County-provided Internet, intranet, and email services, when directed by the CIO to do so.

5.1 Department

A. Ensure that employees are informed of, and comply with, this administrative procedure.

B. Responsible to ensure the appropriate use of department resources, including IT and official employee time.

C. Ensure that this administrative procedure is incorporated by reference into all contracts in which the County is to provide contactors or volunteers with the use of its Internet, intranet, or email services to conduct the County's business, and that all contractors and volunteers are bound to comply with this administrative procedure.

D. Pay the cost of ISP services or remote access connections that it approves for non-networked PCs.

E. Manage the configuration of anti-virus software for non-networked, County-owned PCs, and obtain from DTS any necessary anti-virus software.

F. Through DTS or departmental IT staff, ensure that the operating system on PCs have software updates in accordance with County information technology policies and procedures.

G. A Department head must seek approval from the CIO prior to monitoring or accessing an employee's electronically-stored email messages or computer files, or any other electronically-stored information available related to the employee's use of the County's Internet, intranet, and email services.

5.2 County Employees

A. Keep apprised of the latest version of this administrative procedure.

B. Ensure use of County-provided Internet, intranet, and email services is in accordance with this administrative procedure.

C. Must not access another user's email account without authorization from the department director or the employee to whom the email account is assigned.

D. Obtain department approval prior to acquiring a County-provided ISP connection for a non-networked PC.

E. In accordance with County information technology policies and procedures, obtain approval from the CAO before sending a broadcast email to all, or the majority of, County email users.

PROCEDURE

6.0	Employee	Abide by this administrative procedure as it relates to the use of Internet, intranet, and email services.
6.1	Department	Ensure that all employees are informed of and abide by this administrative procedure.

ISP Connection on Non-Networked Computer

6.2	Employee	Request approval from department for the acquisition of a County-provided ISP connection for a non-networked PC.

6.3 Department

Approve or disapprove of the employee's request for a County-provided ISP connection for a non-networked PC.

Pay the costs of any approved ISP services that result from the employee's request.

Broadcast email

6.4 Employee

Request approval from department for sending a broadcast email to all, or the majority of County employees.

6.5 Department

Request approval from the CAO prior to permitting an employee to send a broadcast email to all, or the majority of, County employees.

6.6 CAO

Approve or disapprove requests to send County-wide broadcast email messages.

Monitoring and Accessing Use

6.7 Department

Determine if there is a legitimate business purpose to monitor an employee's use of County-provided Internet, intranet, and email services, or to access an employee's email messages or computer files.

If there is a legitimate business purpose to monitor an employee's use of County-provided Internet, intranet, and email services, the department head must request in writing to the CIO for approval to monitor an employee's use of County-provided Internet, intranet, and email services or to access an employee's email messages or computer files.

6.8 CIO

Approve or disapprove a department head's request for monitoring or accessing an employee's email messages or computer files.

6.9 DTS

For approved requests, provide appropriate information to the requesting department head.

DEPARTMENTS AFFECTED

7.0 All County Departments.

MONTGOMERY COUNTY ADMINISTRATIVE PROCEDURE

Offices of the County Executive • 101 Monroe Street • Rockville, Maryland 20850

NO. 6-7

PAGE 1 OF 13

DATE 5/4/2005

CAO APPROVAL

TITLE Information Resources Security

PURPOSE

1.0 To establish a procedure that ensures the County's electronic data assets are protected from theft, unauthorized destruction, use, modification, or disclosure.

DEFINITIONS

2.0 Access Point – This is a means of connection between networks, or between a network and a user device. Some examples of an access point are a wireless hub or device, a modem, a cable modem, a DSL (Digital Subscriber Line) connection, an ISDN (Integrated Services Digital Network) line, A VPN (Virtual Private Network) service, and a router or other device with more than one network interface between two or more subnets.

2.1 Computer Security Guideline - A document that defines security procedures and standards, which is located under the on-line address at: http://portal.mcgov.org/dpttmpl.asp?url=/content/departments_intranet/DTS/PolicyProcs/index.asp

2.2 County Information Resources – A Montgomery County-owned, leased, or licensed computer, peripheral, network, system, or software element or package, and information transmitted, received, or stored using a County-owned, leased or licensed computer, peripheral, network, system, or software element or package.

2.3 Department of Technology Services (DTS) - A department in the executive branch that is responsible for automated information systems and telecommunications technology for the County Government.

2.4 Disaster Recovery Guideline - A document that describes the Information Technology steps taken for a disaster recovery, which is located under the on-line address at: http://portal.mcgov.org/dpttmpl.asp?url=/content/departments_intranet/DTS/PolicyProcs/index.asp

2.5 Digital Subscriber Line (DSL) - A family of technologies that provide a digital connection over the copper wires of the local telephone network.

2.6 Extended Network – A permanent or semi-permanent physical extension of the County's computer network to a non-County facility that is used by County and non-County employees to access County Information Resources.

2.7 Incident Response Guideline - A document that describes the policy for handling security incidents, which is located under the on-line address at: http://portal.mcgov.org/dpttmpl.asp?url=/content/departments_intranet/DTS/PolicyProcs/index.asp

2.8 Information – Data stored, processed, or transmitted by or to a computer, Personal Data Assistant (PDA) or any other device.

2.9 Information Technology Staff – An employee who is responsible to deploy, manage, administer, program, maintain or dispose of the County's computers, peripherals, networks, or software. This does not include staff that simply uses a computer, peripheral, network, data, or software to complete a job responsibility.

2.10 Integrated Services Digital Network (ISDN) – Type of circuit switched telephone network system, designed to allow digital (as opposed to analog) transmission of voice and data over ordinary telephone copper wires, resulting in better quality and higher speeds, than available with analog systems.

2.11 Network – Transmission channels and all supporting hardware and software interconnecting the County's computers and peripherals.

2.12 Network Equipment – Goods necessary for network communications, including routers, hubs, switches, network Interface cards, firewalls, and bridges.

2.13 PC – Personal computer.

2.14 Peripheral – Any hardware device connected to a computer (e.g., a monitor, keyboard, printer, Universal Serial Bus device, plotter, disk or tape drive, graphics tablet, scanner, joy stick, or mouse).

2.15 Privileged Account – A logon identification to the network with access exceeding the standard access given to employees.

2.16 Redundant Array of Independent Disks (RAID) – a system of using multiple hard drives for sharing or replicating data among the drives.

2.17 Risk Assessment Guideline - A document that defines how to assess a risk to data or County Information Resource, which is located under the on-line address at: http://portal.mcgov.org/dpttmpl.asp?url=/content/departments_intranet/DTS/PolicyProcs/index.asp.

2.18 Sensitive Information – Any information considered sensitive by law or County policy, including criminal justice, payroll/personnel, client or patient medical information.

2.19 System – A set of hardware and software that processes data in a meaningful way. A relatively simple computer system is a personal computer (PC).

2.20 System Administrator – An employee, either from DTS or another department, who is responsible for assigning and maintaining access rights (approvals) for privileged accounts.

2.21 Virtual Private Network (VPN) – A VPN is a network that uses encryption and other security methods to create a secure network on top of a non-secure and often public network.

POLICY

3.0 An employee must protect information resources commensurate with its level of sensitivity and applicable legal and County policy mandates for that particular type of information.

3.1 An employee must limit private use during his or her access to a County Information Resource, and normally use County Information Resources only to complete his or her work-related responsibilities.

3.2 A County Information Resource must have adequate environmental protection and safety systems, in accordance with manufacturer recommendations.

3.3 An employee may remove a County Information Resource from the County's premises only for business purposes and only upon the approval by appropriate personnel within the employee's department in custody of such resources.

3.4 Information that is critical to the County's operations must have regular backups and off-site storage. A department is responsible for having a critical County Information Resource disaster recovery plan, to provide for continuity of critical business operations and service delivery, in accordance with published DTS operating standards. The department must test the systems covered by the disaster recovery plan on a regular basis.

3.5 An employee and/or a department must follow the requirements listed under Paragraph 4.31 of this administrative procedure to have remote access to County Information Resources.

3.6 A County employee who violates this administrative procedure may be subject to disciplinary action, in accordance with Montgomery County laws and executive regulations, including Personnel laws and regulations, and Ethics Laws, currently codified at Chapter 33, COMCOR Chapter 33, and Chapter 19A of the County Code, respectively, and applicable collective bargaining agreements, as amended. Violation of this procedure is prohibited and may lead to disciplinary action, including dismissal, and other legal remedies available to the County.

3.7 In any contract where a contractor or business partner may have remote access to, or otherwise work on or interface with, County Information Resources, including those situations described below in paragraphs 4.11 (G), 4.12, 4.14 (E), 4.30, 4.31 (E) and 5.1 (C), the following language, or language of similar import, must be included in the solicitation document and the contract, and AP 6-7 must be attached:

This Contractor may be afforded remote access privileges to County information resources, or otherwise work on or interface with County information resources, and must ensure that the County's information resources, including electronic data assets, are protected from theft, unauthorized destruction , use, modification, or disclosure as deemed necessary under the County's Information Resources Security Procedure (AP 6-7). The Contractor must adhere to any and all policies and procedures under, or related to, the County's Information Resources Security Procedure (AP 6-7), which is expressly attached to, incorporated by reference into, and made a part of, this contract.

GENERAL

4.0 DTS must configure and install all access points connected to a County Information Resource.

4.1 DTS must install County network access controls (e.g., firewalls, boundary routers, etc.) to protect County Information Resources.

4.2 DTS will perform periodic (e.g., daily, bi-annual, etc.) security vulnerability audits on all County Information Resources in accordance with this administrative procedure.

4.3 Any Information or Information Resource that is contained in or stored on County Information Resources, or transmitted or received using County Information Resources, is the property of the County and, therefore, is not considered private.

4.4 The following are required to protect the identification and authentication of users of a County Information Resource:

A. Employees must, at a minimum, use identification controls and individual access accounts with passwords, to gain access to a County Information Resource.

B. Employees must not share identification controls.

C. Employees must limit privileged account use to specific functions, e.g. loading software, and may not be used on a continual basis apart from the intended function.

D. Account lockout procedures must conform to County Computer Security Guidelines.

E. DTS must terminate an employee's access to County Information Resources, immediately, when the employee is no longer employed in County service, or when an employee's responsibilities no longer require access to County Information Resources. DTS must terminate a contractor's access to County Information Resources, immediately, when the contractor's services is no longer required. Departments have this same responsibility for computer/device accounts under their control.

F. DTS must test password quality on a periodic basis. If a password is found to be weak as defined in the Computer Security Guideline the user must change the password.

G. Departments must disable any unused network logon ids.

4.5 The following are requirements to protect Sensitive Information:

A. An employee must not store Sensitive Information on a PC, unless DTS-approved PC security software is installed in the PC. A current list of DTS-approved PC security software is contained in the County Security Guidelines.

B. DTS may enable an employee to have access to Sensitive Information, only on the condition that the employee requires that Sensitive Information to perform the employee's responsibilities for the County.

C. An employee who has Sensitive Information stored on electronic media, or in any physical format, such as paper or fiche, is responsible for locking the information in a secure area when not in use, and deleting, reformatting, or shredding that Sensitive Information when it is no longer needed.

D. After using a PC terminal, an employee must not leave the PC terminal while Sensitive Information is displayed on the screen. An employee must never leave Sensitive Information on the computer terminal unattended; if necessary the department must install a screen-locking feature on the PC that blanks the screen until the correct password is entered.

E. The warning banner, as described in the County Security Guidelines, must be displayed on monitors, before employees are granted permission to access the computer system. An employee must have explicit permission from DTS in order to access or configure a computer device. All activities performed on a County Information Resource may be logged.

4.6 DTS requires that an information system joining the County network meet minimum security requirements as defined in the Computer Security Guidelines, unless an exception is granted by DTS.

4.7 The following are requirements when installing software security upgrades on County Information Resources:

A. A department is responsible for applying critical security patches, specified by the software vendor, for computer systems within 30 days after public release. For systems containing Sensitive Information or systems accessible via the Internet, a department is also responsible for applying critical security patches, within seven days of public release.

B. During emergency situations, the DTS Security Office may require that all computer systems immediately receive patches.

C. Departments must apply non-critical security patches to all County Information Resources other than computer systems within 90 days after public release.

D. If, due to incompatibility or other issues, a critical security patch cannot be applied, a department must submit an exception report, in writing, to the DTS Security Office.

E. The DTS Security Office must periodically verify software revision and patch levels for all County systems.

4.8 The following are requirements when using computer viral controls:

A. A department must install and run a DTS-approved, centrally administered, anti-virus application, using a DTS-approved configuration on all Information Resources that connect to the County network. A department must utilize the automatic updates, if available.

B. DTS and departments must protect County Information Resources by using an anti-virus program with virus definition no older than two weeks and having current approved software security updates applied to the County Information Resources.

4.9 The Department of Technology Services will do the following to audit County Information Resources:

A. Audit and review information resources on a regular basis, based on the sensitivity of the information or systems.

B. Log, and keep for a period of at least one year, records of unauthorized attempts to access Sensitive Information.

4.10 A department must install and run a DTS-approved, centrally administered, anti-spyware application, using a DTS-approved configuration on all Information Resources that connect to the County network. A department must utilize the automatic updates, if available

4.11 The following are requirements when accessing a non-County controlled network from within the County's network:

A. The right to use remote access services must be in accordance with AP 6-1, Use of County-provided Internet, Intranet, and Electronic Mail Services.

B. Access to remote access services must comply with the remote network owner's security and use policies.

C. A user that requires, and seeks to obtain, a modem at his/her workstation for remote access must receive approval from the DTS Security Office.

D. Encryption and authentication of any County Information Resource is required, if Sensitive Information is to be transmitted over public phone lines, the Internet, or wirelessly.

E. Sensitive information may not be stored on non-County controlled resources unless the department follows DTS procedures, County Security Policy, and all Federal, State and County laws and policies.

F. All VPN clients or any tunneling devices installed within the County network must be approved by DTS Security Office.

G. In order for a contractor to be afforded remote access privileges, the contractor must follow the same security requirements detailed in this administrative procedure and any other County Information Resource procedures. A department must include the Information Resources Security requirements noted in this administrative procedure in, or attach this administrative procedure to and incorporate it by reference into, any contract to which this administrative procedure applies.

4.12 The following must be met for a contractor or business partner facility to work on an extended network:

A. All network connections between a contractor or business partner and the County must meet the same security requirements detailed in this administrative procedure and the Computer Security Guidelines. The contractor or business partner must agree to implement, comply with, and enforce all County security policies and guidelines. A department must include the Information Resources Security requirements noted in this administrative procedure in, or attach this administrative procedure to and incorporate it by reference into, any contract to which this administrative procedure applies.

B. Failure by contractor or business partner to maintain full compliance with the County's security policies may result in immediate termination of the connection, and may be the cause for cancellation of any contract between the County and the contractor/business partner.

4.13 A department must do the following for the vulnerability, assessment, and remediation of County systems:

A. Conduct risk assessments and remediation on County Information Resources on a regular basis, commensurate with the level of sensitivity of the information, according to the Risk Assessment Guideline.

B. Support DTS scans against common infrastructure, on a regular basis.

C. Remediate vulnerabilities on a timeline commensurate with the associated level of risk. (Refer to Incident Response Guideline).

D. Report all system or network installations to the DTS Security Office, prior to implementation.

E. Comply with County Computer Security procedures established by the DTS Security Office, when installing new software.

4.14 Departments must do the following to ensure the safety of County Information Resources and personnel.

A. Create policies and ensure compliance to physically secure work areas.

B. Locate all new computer and communications centers in an area unlikely to experience natural disasters, serious or man made accidents, and related problems. New and remodeled facilities must be constructed to protect against fire, water damage, vandalism, and other threats that may occur. The location of multi-computer or communications facilities should be selected to minimize risk of damage.

C. Develop computer centers in consultation with DTS and the Department of Public Works and Transportation.

D. Notify the Department of Public Works and Transportation if changes in facilities are needed or if changes to plans are required.

E. A department must include the requirements of this administrative procedure in any contract to which this administrative procedure applies.

4.15 The Department of Public Works and Transportation must do the following to ensure the safety of County Information Resources and personnel:

A. Use environmental controls, including those related to humidity, temperature, and lighting, to protect all equipment.

B. Install fire detection and suppression equipment, as required by County, Federal and State law.

C. Periodically, inspect environment and safety systems by qualified personnel.

D. Use electrical protections on County Information Resources, commensurate with the importance of the County Information Resource.

E. Ensure the area is structurally sound.

F Ensure a physically secure infrastructure envelope exists.

G. Develop computer centers in consultation with DTS.

4.16 Departments and the DTS Security Office must do the following to ensure that access to County Information Resources is secure, by taking measures that include the following:

A Physically restrict unauthorized personnel from accessing County buildings, computer labs, offices, and work areas containing County Information Resources, including related equipment.

B. Permit only authorized personnel to have access to servers and wiring closets.

C. Restrict access to magnetic tape, disk, and documentation libraries to only employees whose responsibilities require access to them.

4.17 A department must do the following when moving or removing County Information Resource equipment owned or managed by DTS:

A. A departmental director or designee must receive approval from DTS to remove County Information Resources, which may occur only for DTS-approved business purposes. A department must provide the reason(s), in writing, for moving or lending the equipment. A department that has received approval to remove equipment so it may be repaired provided the department complies with DTS-approved repair processes and retains a receipt for the equipment from the repair provider.

B. Do not relocate computer equipment without prior authorization from the appropriate DTS management and/or technical support staff.

C. Use a sign-out procedure, approved by information resource owners, for all shared resources.

4.18 A department must do the following when installing copyrighted software:

A. Not make, use or display unauthorized copies of licensed software on County Information Resources.

B. Periodically, take an inventory of all software to determine if the software is properly licensed.

C. If an illegal copy of software is found, promptly acquire a license for the software or delete the software from the system, immediately. Document the discovery, licensure, or deletion of any illegal copy of software found.

4.19 Violation of this administrative procedure may result in adverse consequences, including fines to the County by the Software and Information Industry Association, or an indemnification or disciplinary action against the responsible employee.

4.20 A user of County Information Resources must not disable or modify security measures installed on any computer for any reason, without permission from appropriate DTS staff.

4.21 A user of County Information Resources must be trained in information security awareness, security threats, organizational policy issues, and the security aspects of the specific systems that the employee's department uses.

4.22 A department must do the following when designing or repairing a network server:

A. Place service contracts with the hardware vendor for repair/service for critical production systems, if possible. Contracts must specify response times for service, if possible.

B. Use backup or failover devices for critical network systems, if possible.

C. Place back-ups of County Information Resources at a physically separate, environmentally-controlled facility.

4.23 A department is responsible for the following when backing up County Information Resources:

A. Back-up crucial data and files frequently, and retain at least the last three back-up copies. The backing up of data is to be commensurate with the frequency of change of the data and the importance of recovering the lost data in a timely manner.

B. Back-ups must be at a physically separate, environmentally controlled facility.

C. All media used to store sensitive, valuable, or critical information for longer than six months must not be subject to rapid degradation. This information must be copied to newer media when the time limits suggested by the manufacturer are close to expiration.

D. Additional protections, such as RAID technology and hardware redundancy, should be used for appropriate, mission-critical applications.

4.24 A department is responsible for the following when establishing a disaster recovery plan for its data:

A. Develop a detailed disaster recovery and continuity of operations plan for County Information Resources.

B. A department that wishes to be supported by DTS, in the event of an emergency or disaster, must implement hardware and software policies and related procedures consistent with DTS standards. DTS staff is available to work with departments and offices to ensure compliance with DTS standards. (Refer to the Disaster Recovery Guidelines).

4.25 A department must develop a detailed plan to shut down each device in a computer center quickly, in the event of an emergency.

4.26 A department may be exempt from this administrative procedure under the following conditions:

A. The department must request exemption from this administrative procedure and receive written approval from the DTS Security Office. A detailed reason for the exception must be included, as well as the business purpose for the exception and additional precautions that will be taken to reduce the risk to the County network if the exception is granted. Examples of additional security precautions may include restricting Internet access and eliminating floppy disk and CD drives on the PC, or disconnecting from the County network.

B. A department that complies with the aforementioned section, and includes in its reason(s) for exemption that it has some older computer platforms in use that lack the capability to implement the security procedures outlined in this document. In this event, a department must purchase upgrades or replacements to these computer platforms as soon as possible, and, until this occurs, all Sensitive Information must be moved off these computers.

4.27 Employees may use County Information Resources only as follows:

A. For County business purposes, as provided under Paragraph 3.1 of this procedure and in accordance with AP 6-1, Use of Internet, Intranet, and E-mail Services, employees are responsible for using County Information Resources responsibly and to follow all related policies, regulations, security requirements, and laws.

B. Sign a confidentiality agreement in accordance with any policy, regulations, or laws.

C. Any use of County Information Resources, including the Internet, intranet, email, computers, or peripherals is subject to the County's review, copying, storing, archiving, and monitoring for violation of policies, regulations, and local, state or federal laws.

D. Montgomery County is not responsible for maintenance, damage, or loss of personally-owned computers, data, or peripherals used by employees in the work place.

4.28 An employee must use County Information Resources responsibly and professionally, and must not use County information resources in a manner that violates any federal, State of Maryland, or Montgomery County law, regulation, or policy, including this administrative procedure.

4.29 Employee orientations within the departments must include a requirement that employees take appropriate security precautions to protect County Information Resources, commensurate with the level of the employee's job, and the sensitivity level of the information the employee is required to use.

4.30 This administrative procedure applies to contractors, vendors, and volunteers who connect their computers to the county network. A department must include the requirements of this administrative procedure in any contract to which this administrative procedure applies. In addition all contractors, vendors and volunteers must comply with County Security Guidelines.

4.31 To have remote access to County Information Resources, an employee and/or a department must do the following:

A. An employee must receive written approval from the County Information Resource custodian and the DTS Security Office to have access County Information Resources from a non-County location, such as an employee's home or contractor's network. This written approval will be in an e-mail sent after the VPN request form is approved.

B. Before a department may purchase or install a remote access connection, the department must request and receive DTS Security Office approval, in writing, for the purchase or installation of a remote access connection.

C. Remote access of County Information Resources must be in accordance with AP6-1, Use of County-provided Internet, Intranet, and Electronic Mail Services.

D. Encryption and authentication of any County Information Resource is required, if Sensitive Information is to be transmitted over public phone lines, the Internet or wirelessly.

E. In order for a contractor to be granted remote access privileges, the contractor must follow the same security requirements detailed in this administrative procedure and any other County Information Resource procedures. A department must include this requirement in any contract to which this provision applies.

F. Sensitive Information may not be stored on non-County controlled resources unless following Department and DTS procedures and the County Security Guidelines and all Federal, State and County laws and policies.

RESPONSIBILITIES

5.0 Department of Technology Services

A. Maintain County information security policies appropriate for best business practices relating to the changing information security requirements of an enterprise network.

B. Conduct security scans and vulnerability testing to identify vulnerabilities in the County Information Resource network.

C. Advise departments on information security issues and assist them in the remediation of identified vulnerabilities.

D. Assist departments in the design of County Information Resource networks, to ensure a secure architecture.

E. Identify resources for security awareness training.

F. Function as the point of contact for County Information Resource-related security incidents.

G. Maintain an awareness of County Information Resource security threats and countermeasures.

5.1 Department

A. Become familiar with the County Information Technology Security Administrative Procedure.

B. Provide appropriate employees training to perform County Information Resource-related job functions, in compliance with County information technology security procedures.

C. Incorporate and include this administrative procedure as part of any contract in which the County is to provide a contractor or its agents or employees access to the County Information Resources network.

D. Cooperate with DTS staff in the vulnerability testing and remediation process of department-operated County Information Resources assets.

5.2 Employee

Use County Information Resources for County business purposes and in compliance with this administrative procedure.

PROCEDURE

6.0 Department of Technology Services

Provide departments with security policies and procedures and consulting expertise needed to maintain a secure and available County Information Resources network.

Promote County Information Resources security awareness training.

Scan the entire County Information Resources network periodically for known vulnerabilities and initiate remediation as required.

Provide leadership in resolving County Information Resources security incidents and preventing incidents where possible.

6.1 Department

Enforce employee compliance with this administrative procedure.

Train employees on department specific security policies and procedures.

Assist DTS staff with maintaining the department Information Resources in a secure environment and in compliance with County security policies.

DEPARTMENTS AFFECTED

All County Departments.

APPROVED AS TO FORM AND LEGALITY.
OFFICE OF COUNTY ATTORNEY
BY Richard H. Melnick
DATE 4/25/05

Computer Security Guideline

Department of Technology Services

Revision Information

Effective Date: ___03_/_23_/_2009__

Last Revised Date: __03__/__23_/_2009__

Change History:

Changer/Author	Description/What Changed
Joan Cole	New policy statements to include Encryption for laptop hard drives, flash drives and portable external hard drives. Password requirement for Blackberry and other PDA devices.

Table of Contents

1. SCOPE

The scope of this Computer Security Guideline includes all County owned or controlled computers (PCs, laptops, PDA's, wireless devices, servers, mini-computers, mainframe computers), all County owned or leased buildings, all data stored on those devices, all printouts, disks, tapes, or other media produced by those devices and all licensed software used on those devices. In addition, this Computer Security Guideline includes communications links to contractors and business partners and extensions of the County's computer network.

This Computer Security Guideline applies to all County employees, contractors, volunteers and persons legitimately affiliated with the County government for the efficient exchange of information and the completion of assigned responsibilities.

2. OVERVIEW

This Computer Security Guideline reflects accepted security controls taken from respected security and audit publications and adapted to Montgomery County's technical environment. These data security guidelines and standards have been developed to protect Montgomery County Government's electronic data assets from theft, destruction, and unauthorized use, modification, or disclosure. The loss of these assets could be very costly and disruptive to the County government. In today's computing environment, security controls are a necessity. The citizens of this County expect us to do what is prudent to protect the computing assets purchased with their tax dollars. Data is one of the most valuable assets of the County government. End-user computing dramatically increases the exposure for theft, corruption, loss, and misuse of County information resources since a larger number of people have access to data and data security controls. A significant percentage of direct access storage device capacity is installed outside the Computer Center. Security is an issue that cuts across all computing and organizational tiers. The implementation of security policies and procedures requires cooperation among users, managers, information systems personnel, security, audit personnel and most importantly, support from top management.

Access to the entire County's computing and communication resources is to be controlled based on the needs of the County and used for official County business only. Connection and access to computing resources is controlled through unique user identification (user-ids) and authentication (passwords). Each individual granted this privilege is responsible and accountable for work done under their unique identifier.

Computer users will be given access to a copy of the latest version of the Computer Security Administrative Procedure, this guideline, and the *Internet, Intranet, & Electronic Mail Administrative Procedure*. Individuals must adhere to the policies and are responsible for having the latest version of the Administrative Procedure. Refer to the *Internet, Intranet, & Electronic Mail Administrative Procedure* for additional information related to use of the Internet.

3. RESPONSIBILITIES

All Montgomery County Government computing and communication hardware, software, and data are considered to be "owned" by the Montgomery County Government.

The Department of Technology Services (DTS), in accordance with Montgomery County code section 2-58D, is responsible for protecting the integrity of the telecommunications network backbone, for operation and maintenance and security administration of the "enterprise" servers, mainframe and for maintaining the Computer Security Administrative Procedure and these guidelines. DTS is responsible for insuring that computer connections between County departments and with other government agencies are accomplished securely and as authorized.

Management in each department is responsible for ensuring that these computer security guidelines are enforced on the computing resources in their department. These security guidelines will be enforced for employees as well as for contractors and volunteers. Department management is responsible for providing pertinent information and notifying the DTS Security Team if a serious security breach occurs such as an intrusion, theft, or damage of computing resources. The operation, maintenance and security of de-centralized computing resources is the responsibility of department management in accordance with these guidelines.

The Local Area Network (LAN) administrator or decentralized IT staff is responsible for implementing the computer security guidelines described in this document on the servers in their department. LAN administrators will contact DTS network management for allocation of IP addresses.

As a user of data or computing resources or a custodian of those assets, everyone is responsible for data security.

4. PHYSICAL SECURITY

4.1 Guideline

Physical access to servers, individual PCs, and minicomputers will be protected from unauthorized persons. Personnel will not be put at risk of bodily harm.

4.2 Environmental Requirements and Recommendations:

A safe environment must be provided. Fire detection and suppression, and power and air conditioning are examples of the computer environmental protection and safety systems that must be provided.

- Areas with critical computer equipment must be equipped with fire and smoke alarms, and fire extinguishers.
- Critical equipment should be stored in a location that minimizes or prevents water damage due to leaking or flooding.
- Tall and top-heavy items must be stored in a manner anchored at to prevent damage or physical tipping.
- Items on wheels must have locking mechanisms to prevent rolling.

All equipment is to be maintained in a clean environment that meets or exceeds the manufacturer specifications related to temperature and humidity. Equipment areas should be kept free of obstructions. The cleanliness, environmental protection and safety systems are to be regularly monitored, and periodic inspections by qualified personnel should be scheduled. Electrical protection must be provided. Computer systems should have uninterruptible power supplies (UPS) and/or surge suppressors. All electrical wiring must meet state and local building codes. Preventive maintenance on computer and communications must be regularly scheduled. Preventive maintenance as defined by the manufacturer will help ensure that the risk of failure is minimized.

All new computer or communications centers must be located in an area unlikely to experience natural disasters, serious or man-made accidents, and related problems. New and remodeled facilities must be constructed to protect against fire, water damage, vandalism, and other threats that may occur. The location of multi-computer or communications facilities should be selected to minimize risk of damage. Locating such facilities above the ground floor will minimize the chances of water damage and theft. Kitchen facilities also must be located away from, but not directly above or below computer facilities. Due to potential water damage, restroom facilities should not be located directly above these facilities. Computer facilities should not be located adjacent to an exterior wall to protect the systems from unauthorized electromagnetic eavesdropping and damage from bombs.

DTS can provide the needed facilities more economically than creating a new computer center. If a new computer center needs to be created, contact the manager of the DTS computer center for requirements assistance. Local laws and ordinances must be considered when designing these locations.

4.3 Access to Work Areas:

Access to all buildings, computer labs, offices, and work areas containing computer-related equipment must be physically restricted and controlled. Access to servers and wiring closets must be restricted. Only authorized personnel will have access to wire closet/server areas. Authorized persons may include:

- DTS staff
- Outside contractors hired to work in these areas
- Building services and office staff at locations trained to reset equipment
- Fire and/or rescue personnel

Access to computer equipment must be supervised. Access to offices, computer rooms, and work areas containing sensitive information must be physically restricted. Managers responsible for employees working in these locations must determine the appropriate access controls. All multi-user computer and communications equipment such as fileservers, labs, and wiring closets must be located in locked rooms to prevent unauthorized usage.

Access to Server Centers or Network Operations Centers (NOCs) is restricted. Only employees whose job responsibilities require access to the client server center will be granted access. The supervisor of a server center or NOC is responsible for authorizing entrance and maintaining a list of those authorized to enter the facility.

Access to magnetic tape, disk, and documentation libraries must be restricted to employees whose responsibilities require access to them. The magnetic tape, disk, and documentation libraries housed within the controlled areas of the Server Center require additional precautions. This access is controlled by the supervisor of the Server Center.

Employees are not to permit unknown or unauthorized persons to enter restricted areas as they enter and exit these areas. Physical access controls for County buildings are intended to restrict the entry of unauthorized persons, and employees are expected to help restrict such access.

4.4 Removal of Equipment:

Permission to remove computers or related equipment may be granted only for accepted business purposes. Permission to remove computer equipment must be approved by the director of the department owning the equipment and the reason for lending the equipment must be put in writing stating the reason for which the equipment is loaned. Equipment being removed for needed repairs has implied permission when DTS approved repair processes are followed and a receipt is retained for the equipment.

PC equipment must not be moved or relocated without prior authorization from the appropriate management and/or DTS technical support staff. PC workstations, printers, peripherals, file servers, and electronics are examples of PC equipment covered by this requirement.

All County property must be returned when employees, consultants, or contractors terminate their relationship with County or with a specific work location within the County. It is the responsibility of the supervisor to collect County property from an employee leaving their location. Personnel terminating County employment or moving from one work location to another must inform their supervisor/administrator regarding County property they possess, and building access privileges.

When a computer support employee is involuntarily terminated, due care must be taken. Upon involuntary termination, the employee is to be immediately relieved of all duties and must return all County equipment and information. Their network accounts are to be immediately disabled and they are to be supervised while packing their belongings and leaving County facilities.

A sign-out procedure, approved by department management, must be utilized for laptop computers if there is a shared pool of laptops.

Montgomery County is not responsible for maintenance, damage or loss of personally owned computers or peripherals in the work place.

4.5 Personnel Security

Employees should contact building security if they feel threatened, harassed, or afraid of bodily harm.

Personnel will immediately contact building security if a person:

- becomes unruly
- refuses to leave
- poses a threat to employees, property, or equipment

In the case of an emergency, Montgomery County Police should be immediately contacted or dial 911. This is judgment decision based on the severity of the threat. If in doubt, contact the police first then building security.

4.6 Disaster Recovery

A detailed disaster recovery plan must be developed by each department that has a LAN or mini-computer. This plan will detail procedures to follow in the event of the loss of computing hardware, software and/or data. DTS must prepare, periodically update, and regularly review information technology emergency response plans for the DTS data center and for communications systems. The disaster recovery plan must provide for the continued operation of critical systems in the event of an interruption or degradation of service; must allow all critical computer and communication systems to be available in the event of a major loss, such as a flood, earthquake, or tornado; must prioritize the sequence of critical systems being recovered. This plan must be practiced at least once a year; this practice will include restoring data from backup media to insure that restoration procedures are known and to verify the integrity of the backup media. Each test must be followed by a report, and detail the test results, plus any remedial actions taken. The department can evaluate the effectiveness of the plan and make adjustments as appropriate to accomplish the desired goals. The manager of the DTS data center can provide a comprehensive sample of a disaster recovery plan.

A business continuity analysis will also be conducted by those responsible for their department computing equipment that identifies the procedures that need to be in place in order to ensure that critical operations could continue in the event of a disaster which destroys their computing capabilities. The conditions that warrant a disaster declaration and the persons responsible for this decision will be specified.

Departments wishing to be supported by the DTS in the event of an emergency or disaster must implement hardware, software, policies, and related procedures consistent with DTS standards. DTS staff is available to work with offices to ensure compliance with DTS standards. Backup medium must be erased by following the *Data Backup* section in this guideline.

The communications networks should be designed without a single point of failure whenever possible, such as a central switching center, which could affect the availability of network services.

A backup of system wide critical information and software is to be stored in a physically separate, environmentally controlled facility. This facility is to be at least five miles from the site where original copies reside. Additionally, all current supporting materials such as manuals, charts, and diagrams needed for disaster recovery will be housed at the same facility. Supporting materials include anything required by County departments or units that are necessary to maintain day-to-day mission critical operations until recovery. Contact the DTS data center manager for information on the facility used by the data center for backups.

4.7 Emergency Shutdown Procedures

A detailed plan will be developed by each department with their own LAN or Mini-computer to shut down each device in a computer center quickly in the event of an emergency. Emergencies can include fire, loss of environmental controls, computer virus outbreak, natural disasters, etc. The goal is to preserve County resources in an emergency without subjugating the operator to undue risk. Contact the DTS data center manager for a sample of this plan. The DTS security manager or the director of the affected department can make this determination and contact the appropriate department management personnel to implement the emergency shutdown procedures when warranted by the circumstances. This kind of emergency will require every effort to shut down the computing equipment. Unplug the equipment from the County network if shutdown is not possible.

5. DATA SECURITY

5.1 Guideline:

Employees that are permitted access to computer systems must follow guidelines in order to insure that restricted access is maintained. Users of the computer systems will only have the minimal access needed to perform their tasks. Attempts to bypass security procedures to gain unauthorized access to computer resources are unacceptable and may result in disciplinary action. See section 3 paragraph 5 for information regarding disciplinary action.

5.2 Password and User-id Information:

Strong passwords will be used to protect access to County networked computer systems (LANs, mini-computers, PCs. Unused and default or installation user-ids will be disabled. Use of powerful user-ids such as those with system administrator attributes will be restricted.

Passwords provide a basic first-level security for restricting access to computer resources. To protect County computer resources properly, passwords are required to access all networked computer systems. Passwords will be simple enough to memorize but unique enough to remain secret. Passwords will not be attached to a terminal or other public place where they are easily compromised. Passwords will not be associated with the current date or a person's name, hobby, or family. Good passwords are not found in the dictionary, contain numeric as well as alphabetic characters, and will be at least eight characters in length. Passwords will not be imbedded in user’s automatic sign-on procedures unless approved by that department’s management for procedures where it is required. Passwords cannot be changed in less than 2 days.

A maximum of ninety days between password changes is required for network, server and mini-computer access. The change interval for power on passwords for PCs, if used, is at each department’s discretion. Where possible, password change will be controlled automatically by security software. Passwords will be individually maintained to ensure confidentiality and individual accountability. Passwords will not be shared with others. If multiple people must share a user-id and password for a sound business reason, refer to the exception procedures in section 8 of this document. If it becomes necessary to give your password to a technical person to fix a problem you are experiencing, the password will be changed immediately after the problem is solved. An account will be suspended after no more than five invalid password attempts in a given day and remain suspended until an administrator can reactivate it. Passwords will not be reused for at least four password cycles. A user-id will be suspended after twelve months of non-use.

Access to computer resources will be terminated immediately for employees who leave County employment or when their responsibilities no longer require them to access those resources. Access will also be terminated immediately for contractors no longer requiring access to County computer resources. Department coordinators are responsible for deleting user-ids of people who have terminated, transferred out of the department, or no longer require computer access. If the department coordinator does not have access rights in order to remove or disable the account, then the coordinator must contact the DTS Security Office and E-messaging Directory Services Team.

Computer system security will prevent a user-id from being logged on in more than two different places at the same time. Just one user-id per computer platform will be assigned to an individual. System privileges, such as supervisory or system administrator attributes are sensitive and are restricted to designated LAN or minicomputer system administrators. When the use of sensitive system privileges is necessary by others (for example, during an on-site visit by field service engineers), the privilege will be immediately removed or the user-id disabled after the user is finished with the specific task.

DTS will test password quality on a periodic basis. If a password is found to be weak, the user will be required to change it.

5.3 PDAs/Blackberry Password:

All County issued Personal Digital Assistants (PDAs) or Blackberry devices configured to communicate with County network resources must be password-protected. Enterprise-wide system policy will enforce this policy when device is not in use or after 30 minutes of inactivity.

5.4 Protection of Sensitive Information

Sensitive information includes criminal justice, payroll/personnel, client or patient information and any other data considered confidential by law or departmental policy. Sensitive information will not be stored on a PC unless PC security software has been installed on that PC. Sensitive information should be stored on the mainframe or network server where better security is available to protect the integrity of this information. Access to this information will be restricted to those who have to use it. Examples of information that will be protected from unauthorized access include: word processing documents containing sensitive material, which can be locked (password protected); source code for programs, which can be protected using a source code management tool; databases, which can use built-in security controls; and production files downloaded from the mainframe or server, which can be protected in a directory where limited access is permitted.

Sensitive information stored on computer diskettes, tapes or printout will be locked in a secure area when not in use and deleted, reformatted or shredded when no longer needed.

The same level of security will be maintained across the various computer platforms (mainframe, mini, LAN or individual PC). If a sensitive file located on the mainframe computer is downloaded to an individual PC, that information on the PC will be protected from unauthorized access in an equivalent manner as it is on the mainframe.

PC’s and terminals will not be left unattended with the results of a query containing sensitive information displayed on the screen. If this is necessary, a screen locking feature that blanks the screen until the correct password is entered will be used. Sensitive printouts will not be left on an unattended printer.

Special care will be given for laptop or portable PC's. If possible, sensitive information will be stored on diskettes rather than the hard drive and in a separate secure location from the laptop. Some sensitive information may need to be encrypted in order to ensure adequate security. A power on password will be used. If the PC is lost or stolen, departmental security personnel and the DTS Security Team will be notified immediately, and a complete accounting of what was on that PC will be made.

If possible, unauthorized attempts to access sensitive information will be logged and kept for a period of at least one year. This is information that may be used as evidence in a criminal proceeding and must be protected.

Do not disclose user-ids, passwords or other sensitive information to anyone without verifying their authorization to have this information.

The following statement is wording that will be displayed to users before they are granted computer access. This warning banner will appear each and every time that someone logs into a County computer:

UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action and may be reported to law enforcement. There is no right to privacy on this device.

5.5 Data Backup:

Data and files that are crucial to the department's operations will be backed up and the retention of at least the last three copies is highly recommended. The frequency of backup is to be commensurate with the frequency of change and the criticality of recovering the lost data in a timely manner. Some data may need to be backed up daily; monthly backups in other cases may be sufficient. When possible, backups will be automated and take place during off-peak hours.

All archival back-up data that is stored off-site must be listed in a current log that shows the date when the information was last modified, as well as the content of the information. All media used to store sensitive, valuable, or critical information for longer than six months must not be subject to rapid degradation. This information must be copied to newer media when the time limits suggested by the manufacturer are exceeded.

Offsite storage facilities will be utilized for copies of backup files containing programs, data or transactions representing current County business that, if lost or destroyed, would be difficult or impossible to recreate. All backups will be retained a minimum of four weeks and at least two copies will be kept in offsite storage. Longer retention periods should be considered based on business requirements. Offsite storage facilities will also be utilized for files containing data with retention requirements imposed by county, federal or state government. Magnetic storage media provided by the offsite storage or disaster recovery facility for the purpose of restoring Montgomery County information will be thoroughly erased after being used. This may be done by programs designed to erase sensitive information or by reformatting the media at least 7 times.

Additional protections, such as mirror disks, RAID technology, and hardware redundancy should be used as appropriate for mission critical applications. Contact the DTS data center manager if you need assistance in setting up backup/restore procedures or need offsite storage procedures

5.6 Virus Control

Virus controls are necessary to prevent the spread of computer viruses to other computers in the network. Virus eradication can be very time consuming and result in the loss of service to the citizens of Montgomery County.

Software not purchased by the County (e.g. software from bulletin boards, software from home computers or any other computer or network), when allowed by County and department policy, will be checked for viruses before use. This includes diskettes, CD-ROMs and information downloaded from the Internet or other on-line services. Information downloaded to the hard drive will be checked immediately upon completion of the download. Diskettes and CD-ROMs received from other departments or agencies or from companies doing business with the County will be checked before use.

All those responsible for departmental computer resources will update those resources with anti-virus signatures on a minimum weekly basis and upgrade to the most current anti-virus release as it becomes available. All PC’s and servers that are connected to the county network must have DTS approved, centrally administrated anti-virus software installed and running using a DTS approved configuration. Automatic updates will be utilized if available. Contact the DTS Client Computer Services (DCM) if information is needed on anti-virus software. When DTS issues a security alert and specifies that virus signatures must be updated immediately, those responsible for departmental computer resources must comply.

5.7 Software Security Upgrades

Vendors publish patches and upgrades to their software when they discover security flaws that could allow computer security to be compromised. The DTS Security Team may provide information about enterprise software security issues and patches as available and appropriate.

Because these flaws pose a significant threat, critical security patches for internal computer systems must be applied in a maximum of 30 days after public release. For systems containing sensitive information or are accessible via the Internet, critical security patches must be applied within 7 days of public release. Automatic updates will be utilized if available. If alerted of a specific critical threat that could severely affect County resources, the DTS Security Office may issue a mandatory, short time frame alert to computer administrators to patch specific computer resource in order to reduce the risk of network down time.

Non-critical security patches must be applied to all systems within 90 days of public release.

If, due to incompatibility or other issues, a critical security patch cannot be applied, an exception report must be sent in writing to the DTS Security Office.

On a regular basis, the DTS Security Office will verify software revision and patch levels for all County systems. Refer to the *Vulnerability Assessment and Remediation* section for details.

6. SECURING PORTABLE DATA

6.1 Guideline:

The widespread use of portable computing devices or PDAs, such as the Blackberry, iPods, USB flash drives, etc. has also increased exponentially the threat of theft or loss of sensitive data. The goal is for the County to protect all sensitive data at rest or in transit

6.2 Laptop Hard Drive Encryption:

All primary laptops are supported by the Desktop Computer Modernization (DCM) program and are required to have hard drive encryption. All secondary departmental laptops assigned to specific users must also have hard drive encryption. All secondary laptops not assigned to an individual (shared) will not be required to be encrypted due to operational impacts. Therefore, no County data may be stored on shared laptops. Instead, data used on shared laptops must be stored on secure USB Flash drives.

6.3 USB Flash Drive Encryption:

County requires the use of encrypted USB flash drives. Department Directors must decide who can have such devices; what data will be allowed on these drives; and must cover the cost of acquisition.
For Non-Sensitive Data – Standard off the shelf USB flash bundled with 256 bit AES encryption must be used. For Sensitive Data – Standard off the shelf USB flash bundled with higher levels of encryption and with self destruct function must be used.

6.4 Portable/External Hard Drive Encryption:

Portable/ External Hard drives must be kept in a locked cabinet or drawer/office and must be encrypted if removed from County facilities. Department Directors must decide who can have such devices; what data can be stored on these drives; and enforce either physical security or require a device that has encryption.

7. NETWORK SECURITY

7.1 Guideline:

Access to or from the County network is only permitted for authorized employees and other County approved agencies.

7.2 Remote Dial-in Access to County Computer Resources:

Access to remote network services will be in accordance with the *Internet, Intranet, & Electronic Mail Administrative Procedure*. Approval from the department management and the DTS Security Office will be obtained if a user requires a modem at their workstation for remote access. Modems attached to PC's that are connected to a County network can be very risky and will not be authorized unless DTS-approved security measures are implemented. Unauthorized modems attached to PCs or servers that are connected to a County network are prohibited. If remote access from a County owned PC using an attached modem is required, that PC will be disconnected from all LANs or networks. Refer to the *Internet, Intranet, & Electronic Mail Administrative Procedure* document.

7.3 Access from Remote Networks to County Computer Systems

Access from a remote site to any Montgomery County computer resource will be approved by the employee's Department head or designee and by the DTS Security Office. All remote access systems used to access County computing resources will be approved by the DTS Security Office prior to purchase, installation, or connecting to County resources. Access and security system information must not be disclosed to any 3rd party.

Employees who need remote access to any County computer resources will submit a request in writing to the DTS Security Office stating what the access is to be used for, how long the access is required, and approval from the responsible department official. Contact the DTS Security Office to obtain information and approval for secure remote access options including, but not limited to, VPN, and wireless methods. Modems attached to County computer systems that allow remote access is not an approved remote access method. The list of authorized remote access users will be reviewed periodically by the LAN or mini computer administrator to determine continued need for such access and accuracy of the list. If remote access is no longer required, that access will be terminated.

LAN and mini computer administrators will maintain a log of unsuccessful attempts to access County computers. This log will be maintained for one year.

Encryption of any County-owned data is required if it is to be transmitted over public phone lines, the Internet, or wirelessly. County approved remote access solutions already use encryption.

7.4 Contractor Remote Access

All contractors will meet the same security requirements detailed in this and all other related County documents. The contractor will agree to, and is responsible for, maintaining compliance with all County security policies. Virtual Private Network (VPN) is the current approved remote access method. The sponsoring Department head or designee and the DTS Security Office will approve the remote access request.

The department whose contractor requires remote access to the County's network will present a written justification to the DTS Security Office. All plans for establishing remote access will be approved by the DTS Security Office in advance of implementation. These plans will include at least the following:

Type of access
When and how long access will be required
Security procedures (how contractor access will be controlled)

All contractors requiring access will sign non-disclosure statements and agree to abide by all County security policies and procedures prior to receiving access.

7.5. Extended Networks

Extended Networks are permanent or semi-permanent physical extensions of the County's computer network to a non-County facility and used by non-County employees to access County computer resources.

All network extensions to a contractor or business partner facility will meet the same security requirements detailed in this and all other related County documents. The Contractor/Business Partner (C/BP) will agree to, and is responsible for, maintaining compliance with all County security policies.

The Department requesting the extended network will present a written justification to the DTS Security Office for granting a C/BP access to the County's network from a remote location.

The C/BP will provide a secure link (e.g., T-1) between the C/BP site and the County's Computer Center. All plans for establishing a link will be approved by the DTS Security Office in advance of installation. These plans will include the following:

Type of connection
How long connection will be required
Hours of operation

Number and type of workstations and servers at remote location
Physical security plan
Security Procedures (including keeping all security systems up-to-date)
Anti-virus procedures
Whether Internet access is required for any workstations
The process of disconnecting the C/BP once the connection is no longer needed

All material submissions mentioned above will be submitted by the Contractor / Business Partner to the County Department requesting the extended network, which will coordinate reviews and approvals with the DTS Security Office.

The C/BP will maintain all security provisions, detailed in this guideline, while the remote location is connected to the County network. All employees that have access will sign non-disclosure statements, receive security training, and agree to abide by all County Security Policies and procedures (sign County security agreement), prior to receiving access. All training materials will be approved by the DTS Security Office in advance.

A list of employees with authorized access will be kept up to date and provided in a monthly report to the DTS Security Office. Requests for additional staff access will be approved by the DTS Security Office or County contract administrator prior to granting the access.

The C/BP will permit the DTS Security Office to inspect the remote location without notice, at any time. This may include technical security scanning of the C/BP network segment and any system connected to it.

The C/BP network segment, defined as all workstations, servers, and network equipment connected to the County, will not also be connected to any other network (including the C/BP own internal network). Remote access to the C/BP network segment will NOT be permitted; dial-in or dial-out will not be allowed.

Failure to maintain full compliance with the County's security policies will result in immediate termination of the connection, and may be cause for cancellation of any contract between the County and the C/BP.

7.6 Vulnerability Assessment and Remediation

System/network administrators need to have a vulnerability assessment performed against their assets on a bi-yearly basis. All aspects of this guideline will be evaluated for risk assessment. The security manager will determine the exact schedule. The security manager may also define any additional security assessments other than those described here. In cases where networks reside behind firewalls, multiple assessments should be conducted from both the internal and external sides of the firewalls.

The security manager will be responsible for conducting scans against common infrastructure. The security manager may also conduct scans at random intervals provided that this activity doesn't interfere with business operations. In cases where loss of services might occur, the security manager will coordinate with the appropriate administrators/authorities prior to the assessment.

System/network administrators will only be allowed to scan segments that they're responsible for. Also, the security manager will determine what signatures and scanning methods will be allowed. If sufficient controls do not exist, then the security manager will conduct a scan on behalf of the administrator.

As a general rule, if a vulnerability assessment reveals high-risk vulnerabilities, administrators will have one week to make appropriate changes. Medium-risk vulnerabilities will be addressed within one month. The security manager will coordinate with administrators to adjust this timeline as necessary. If no working patch or configuration change exists or if it will cause an extended or re-occurring stop to business operations, the security manager will evaluate any alternatives or provide a waiver. If high risk vulnerabilities are not remediated within the allotted time, the system may be disconnected from the network. In any case, the security manager will be available to assist administrators in developing remediation solutions. Notify the security manager with results of the vulnerability assessment.

All system or network installations must be reported to the security manager prior to implementation. This should include the following:

New or changed network access points (RAS, VPN, wireless, etc.)
New or changed network segments
New or changed business applications

New or changed application/network servers

New installations must meet County Computer Security Administrative Procedure and be scanned for vulnerabilities using tools approved by the DTS Security Office prior to implementation.

7.7 802.11 Wireless Access

All wireless access points must be approved by the network manager or the security manager. A secure setup on these devices is critical and must be performed by the network team. All other wireless access points connecting to the County network are not permitted. Any existing wireless access points not setup by the network team must be disconnected immediately and the network manager notified to secure the wireless access appropriately.

8. CONDUCT AND USE

8.1 Guideline:

County computer systems should only be used in a legal manner.

8.2 Use of County Computer Resources

All use of computer facilities, networks, and technology resources are for County business purposes. Each user of these technology systems is accountable for using these systems responsibly, following all policies, regulations, security requirements, and laws. *Including the Montgomery County Personnel Regulations 2001 Section 5. Any Employee in violation of the aforementioned regulation will be subject to appropriate disciplinary action.*

As such, all electronic mail messages, files on personal computers or servers, or any information stored on or transmitted by County computers are subject to be reviewed, copied, stored, archived, and monitored for violation of policies, regulations, and local, state or federal laws. *Such employee shall be responsible for appropriate use of all County systems including the transmission to and from the County systems during work and non-business time.*

8.3 Adherence to Software Copyrights

No unauthorized copies of licensed software may be made or used. It is a violation of copyright and trade secret laws and licensing agreements to make or use unauthorized copies of any licensed software. An inventory of all software will be made periodically to determine if the software is properly licensed. Automated tools such as software metering may be used to ensure compliance with license agreements. If illegal copies of software are found, they are to be deleted from the system immediately or properly licensed to protect the County from litigation. This discovery and deletion will be documented.

8.4 Security Measures

Users are not to disable or modify security measures installed on any computer for any reason without permission from the appropriate staff. Security measures include such things as menu software, operating systems settings, and anti-virus software. If it is necessary to disable security to perform a hardware or software installation, security measures must be reactivated when installation is complete.

9. EXCEPTIONS

9.1 Guideline:

Exceptions to any of these guidelines must be approved by the department management and the DTS Security Office. Exceptions will be directed to DTS Security Office by departmental management, in writing or via email, for prompt consideration. A detailed description of the exception will be included as well as the business purpose for this exception and what additional precautions that could be taken to reduce the risk to the County network if the exception is granted. An example of additional security precautions may include restricting internet access and eliminating floppy disk and CD drives on the PC or disconnect from the County network.

There are some older computer platforms in use in the County which lack the capability to implement some of the security procedures outlined in this document. Upgrades or replacements to these computer platforms will be purchased as soon as possible and until this occurs all sensitive information will be moved off these computers. These system exceptions must be documented in writing to the DTS Security Office.

10.0 Guideline Updates

10.1 Guideline:

The Computer Security Guidelines will be modified on as needed basis to reflect changes in our computing environment and deployment of new technologies. Updates or changes to this document will be communicated to County employees via e-mail and revised version will be posted on the County Intranet site.